Technology Control Plan Guidelines

SECURE AND GLOBAL RESEARCH
COLORADO STATE UNIVERSITY

Secure and Global Research
Office of the Vice President for Research
Colorado State University
Phone: (970) 491-7194
E-mail: vpr_export_control@mail.colostate.edu

General Overview

A technology control plan is meant to outline the procedures and infrastructure that you have in place to keep controlled information, technology or equipment from being shared without appropriate authorization. This plan can help your lab understand what needs to be protected, and how. Also, it will serve as certification to the sponsor and the university of providing appropriate security for controlled items and information.
Some of the most common reasons for control are:

- Receiving controlled information or items from a sponsor
  - (examples: Controlled Unclassified Information (CUI), proprietary or sensitive export-restricted specifications or parameters, controlled equipment or materials)
- Restrictions within a contract
  - (examples: publication restrictions, nationality restrictions, DFARS and some clauses related to security and data sharing)
- Producing restricted research results or technology, information, materials or equipment
  - (examples: developing or fabricating restricted items, increasing pathogenicity of select agents or certain pathogens, developing restricted software or data)
- Owning and operating and/or developing restricted equipment
  - (examples: advanced lasers, unmanned aerial vehicles (UAVs), space-related equipment, military end-use items)

Each plan is unique, and may incorporate different portions of a variety of regulatory requirements. By establishing a comprehensive overview of your lab first, we will be able to tailor smaller parts of the plan for any new or changing requirements over the course of one or multiple projects.

To do this, we will establish a Lab Technology Control Plan that describes the general security baselines of your lab. This will include location, general physical and IT security, general research field and lab equipment.

In addition to the general Lab TCP overview, for **controlled projects, we will identify**

(a) reasons for control
(b) personnel working on the project
(c) any additional considerations

Lastly, we will identify whether any overlap between the specific reasons for control, personnel and additional considerations require applying for a federal license. In case that is true our office, Secure and Global Research (SGR), will work with you directly and take the appropriate steps to procure all the required documentation and approvals to keep your research moving forward.

The following guidelines walk through each section of our technology control plan to give you an idea of what sort of information is being requested, and some guidance of how to answer.

Section A – General Lab Information

- **General Research Focus** – This does not need to be specific to any sponsors or funding. This will give us a general idea what sort of research you do. Think of this as the brief, general overview blurb you might put on your lab website.
- **Technology Control Plan Type** – The default for this section is "Lab." Some researchers will complete a control plan for only a single piece of equipment, or a specific visitor, but most researchers who work in an area that includes restricted technology or items will have more than one project that will fall under export controls. If you are unsure how to answer this piece, choose "Lab."
- **Export Control Jurisdiction** – The default for this section is "Multiple." Some labs may already know that most of their research falls under a certain jurisdiction. This will be verified by SGR before signature. If you know this answer, feel free to choose the appropriate regulations. If not, choose "Multiple."

> **ITAR**: International Traffic in Arms Regulations (link)
> **EAR**: Export Administration Regulations (link)
> **OFAC**: Office of Foreign Asset Controls (link)
> **OTHER**: International Treaties, Controlled Unclassified Information Categories, etc.
> **MULTIPLE**: Regulated by more than one agency or regulation, or unknown

- **Signatures** – Please enter the name of the appropriate Department Head. Otherwise, information in numbers 12-15 can be left blank until the plan is completed. This will be routed by SGR.

Section B – General Lab Physical Security

- **Building Location of Controlled Projects/Information** – This may be the same information as listed in Section A, depending on how centralized your lab is.
- **Building Proctor** – Find the Building Proctor for your building. If there is not one listed, please include the individual that generally handles building proctor duties, or the PI.
- **Physical Location** – Include an appropriate snapshot of the building floorplan where your lab is located. You can search here. If there is not a good way to crop and include the floorplan, include it as an attachment, and note that in the textbox.
- **Physical Security** – Describe the security measures within your lab. This is especially important if you share lab space with another research team, or store equipment or do research in an open area. As long as your lab access is maintained by CSU, include the following statement: *Building security is to the CSU standard as described in CSU Building Access, Security and Keys Policy 6-6030-007.*
- **Conversations** – Describe how you protect sensitive information through conversations. This is usually by listing the conference room, or enclosed lab space that is used for meetings. If you use additional conversation methods often (Skype, eg.) you can address that here. An example: *Restricted conversations will take place in [room number] and be limited to personnel who are covered under this technology control plan. If lab meetings take place over Skype, they will take place over a secured network.*

Section C – General Information Technology Security

For an export-controlled project, the information received, created, stored, and transmitted during the conduct of a research project should generally be considered "restricted data" as defined by the CSU Information Technology Security Policy. Under this definition, the information should not be publicly accessible, and should be protected by relevant security controls, so that confidentiality and integrity of data is maintained.

- **Data Storage** – Address the location and technology involved in project data storage. If storage is local to CSU, describe how access is controlled (e.g., a departmental shared drive accessible only to project team members); if storage is cloud-based, identify the vendor and how security features are set.
- **Portable Devices** – Briefly describe portable computing devices used in your lab, who owns them, and who has access.
- **Physical Systems** – This will be a very basic answer. Consider: *Screens are locked when computers being used to access/process controlled information are not in use by authorized personnel.*
- **Encryption** – If you commonly use any encryption outside of any standard CSU encryption, please list it here. Otherwise, answer N/A.
- **IT Contact** – This should be your go-to department IT professional that you would contact in the case of a computer issue.

Note: *If Controlled Unclassified Information clauses are called out in your contract, make sure to check the Yes box in Section II of the* ***addendum*** *so we can refer the question to ACNS Information Security. These security measures will differ from your general lab IT security. More information about CUI can be found on the Secure and Global Research website.*

Equipment List

Please list all equipment within your lab that you are aware is export controlled. Identified items should be labeled with a Capital Asset Management tag that is coupled with a yellow Restricted Use / Export Controlled tag. If they are not yet tagged appropriately, please note that in the CAM Tag# column.

NOTE: For the beginning stages of establishing a lab TCP, this section can remain blank. We don't expect each lab to know all of the restricted or potentially restricted equipment. We will work with you, your lab, and the CSU Capital Asset Management team to evaluate what types of equipment you have in your lab, and what might be restricted. If you have an individual within your department, lab or team who specifically handles equipment purchases and maintenance, please put their name and contact information in this section. If not, please leave blank.

Specific Project Addendum

Section I – General Project Information

The addendum portion(s) of the plan should be specific to a sponsored project, piece of equipment, software package, technology or international visitor (research internship, for example). These portions are in addition to the general lab information, and will be more specific and applied. Often the PI or research staff will not know the answers to some of the regulatory requirement questions. Those will be completed by the SGR office.

These guidelines describe the pieces of information that are **required** from the PI or research staff for SGR to begin constructing the appropriate technology control plan language.

- **Project Start/End Date**
- **Any/all identifying number(s) (53-account, proposal number, award number, or other), if applicable.**
  The items in number 9, 10 and 11 can be modified to more directly address the specific situation
- **Sponsor (if this is a sponsored project)**

Note: Sometimes the easiest way to convey project details is to provide your Request for Proposals (RFP), Proposal (including Scope of Work, Budget, and Deliverables/Outcomes), and Contract Documents. Feel free to submit these documents in lieu of or along with completing the addendum document. We will follow up with questions, if necessary.

Section II – Summary of Project and Control Requirements

Description of the Project – Include enough detail to identify the key reason(s) for control. For example, if you are working on a project funded by the Department of Defense on a dual-use civilian and military item. This may look very similar to your Statement of Work.

Subcontracts – Identify whether or not you are working as a subcontractor, or plan to subcontract out to another entity. There may be flow-down language and/or more information from beginning with the prime sponsor, or requirements that we will clearly address within our subcontracts.

Section III – Dissemination and Publications

Publications – Include your intended dissemination and publication plans. How do you plan to share this data? This includes public presentations, etc. If you need room to explain, please use the explanation box under Section III, 2.

Students Thesis/Dissertation – It is very important to coordinate with the Graduate School as early as possible to avoid any delays or disapproval for student thesis research if this restriction applies. If so, please provide as much detail as you know in the explanation box under Section III, 2.

Section (IV) – Specific Project Personnel

All Project Personnel – List everyone who will be working with this project, equipment or technology. If you do not have details on personnel citizenship, we suggest that you submit with that information omitted to get the review process started. Depending on the reasons for control, US-citizenship may or may not even be relevant. However, before signing the final document, we will ask you to complete the personnel section for your research team.

Questions?

SECURE AND GLOBAL RESEARCH
COLORADO STATE UNIVERSITY

Secure and Global Research
Colorado State University | 309 Johnson Hall
2001 Campus Delivery | Fort Collins, CO 80253-2001
Office (970) 491-7194

Scot T. Allen, Ph.D.
scot.allen@colostate.edu
(970) 491-1563

Rich Wright
rich.wright@colostate.edu
(970) 491-2927